(12) UK Patent Application (19) GB (11) 2 368 147 (13) A

(43) Date of A Publication 24.04.2002

(21) Application No 0014184.6

(22) Date of Filing 09.06.2000

(51) INT CL[7]
G06F 1/00 // G06F 17/30

(52) UK CL (Edition T)
G4A AAP

(71) Applicant(s)
Ali Guryel
30 Hawthorn Road, Bickley, BROMLEY, Kent, BR1 2HH, United Kingdom

(72) Inventor(s)
Ali Guryel

(74) Agent and/or Address for Service
Brookes Batchellor
102-108 Clerkenwell Road, LONDON, EC1M 5SA, United Kingdom

(56) Documents Cited
WO 01/99019 A1 WO 01/92997 A2
WO 01/50391 A1 WO 01/37171 A1
I/S Analyser Case Studies, March 2000, "Shawnee Mission School District portal supports schools, parents", Vol 39, pages 14 to 16

(58) Field of Search
UK CL (Edition T) G4A AAP
INT CL[7] G06F 1/00 12/14 17/30
ONLINE: WPI, EPODOC, PAJ, INSPEC, IBM TDB, Internet

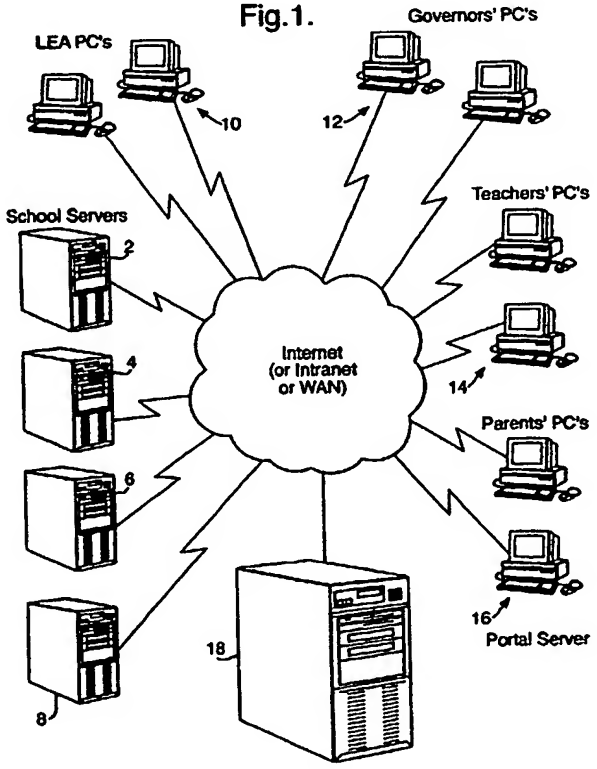
(54) Abstract Title
Access control system for network of servers via port

(57) A distributed database system, in which information is held on a plurality of servers in different physical locations, each having a connection to the internet, and an access portal, also connected to the internet, which is adapted to receive incoming enquiries intended for the servers, to authenticate each enquiry, to identify the appropriate server and to establish a connection with it, once the enquiry has been authenticated.

Communication can be routed through the portal so that there is no direct communication between the originator and the server.

In an embodiment, the database system can be used as an educational network comprising a plurality of servers at different educational establishments holding information relating to students.

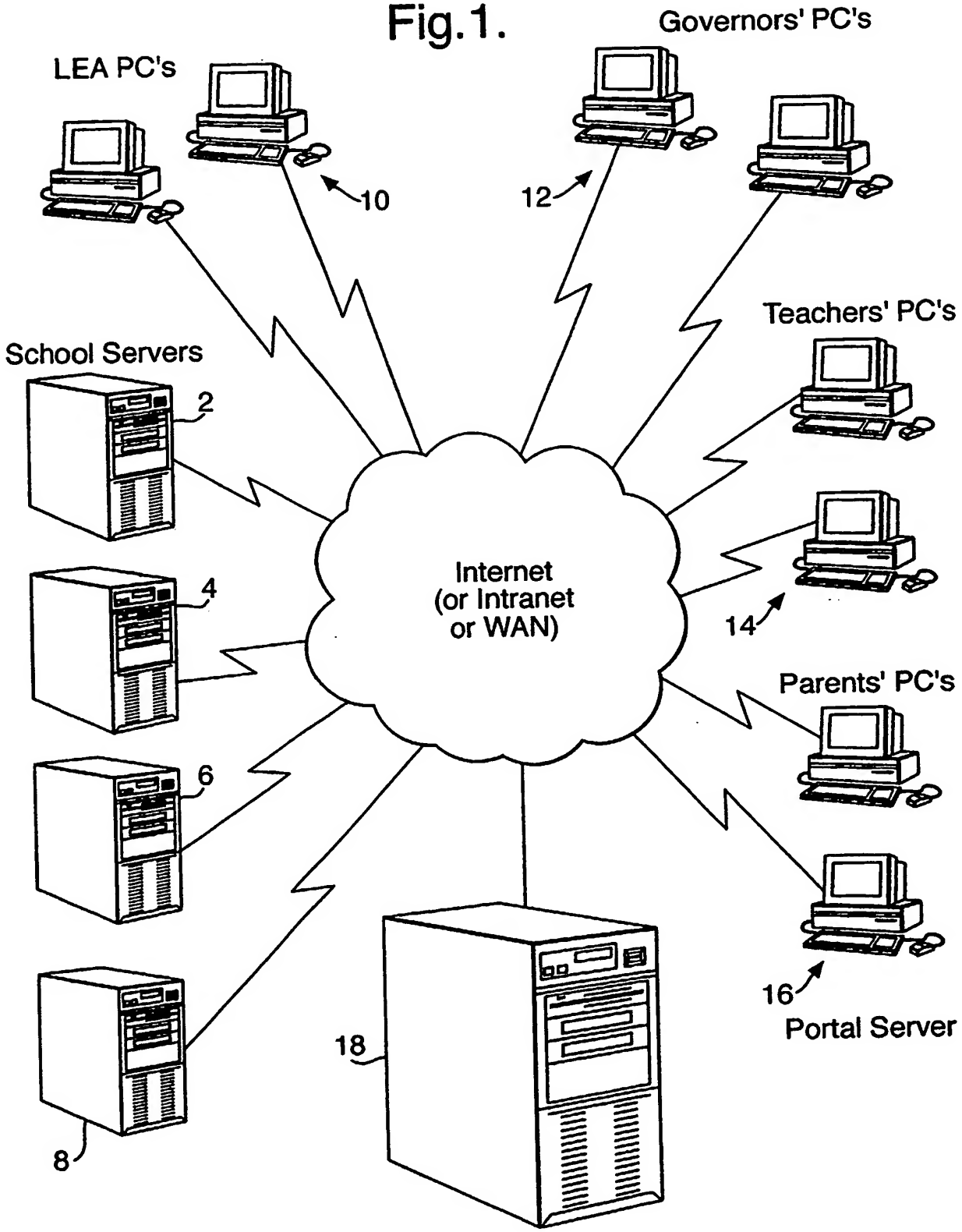
Fig.1.



The claims were filed later than the filing date but within the period prescribed by Rule 25(1) of the Patents Rules 1995.

GB 2 368 147 A

Fig.1.


Governors' PC's
LEA PC's
10
12
Teachers' PC's
School Servers
2
Internet
(or Intranet
or WAN)
4
14
Parents' PC's
6
16
Portal Server
18
8

"Access Control System for Network of Servers via Portal"

This invention relates to data network systems, and in particular, to networks in which a plurality of computers are connected together, by means of a publicly accessible network such as the "internet".

In certain types of such systems, it is necessary to hold information on widely distributed database servers, and for security reasons, it is also required to control access to each server, in order to ensure that unauthorised users do not gain access to confidential information.

Accordingly, the present invention provides a distributed database system, in which information is held on a plurality of servers in different physical locations, each having a connection to the internet, and an access portal, also connected to the internet, which is adapted to receive incoming enquiries intended for the servers, to authenticate each enquiry, to identify the appropriate server and to establish a connection with it, once the enquiry has been authenticated.

Preferably, when the enquiry has been successfully authenticated, a token is passed to the originator, and to the appropriate server, so that the server can confirm that the enquirer is properly authorised, and a direct connection is then established between the two.

Alternatively, when the enquiry has been authenticated, the access portal forwards the request to the server, and the response is routed back to the enquirer, via the access portal, so that there is no direct connection between the enquirer and the server.

The system of the invention is particularly useful in applications where the individual distributed servers are not particularly powerful, and do not have great bandwidths. The access portal is used to control the access to the servers, and the routing of the requests to them, while the other servers by default are set to respond only

to the portal server and to reject all other access requests from any other source. Hence it is only necessary for each server to run a relatively simple access control program, whilst the access portal handles the more complex tasks of authenticating the requests, and routing them to the desired destinations.

One example of an application of the system of the present invention, is an educational information network, in which information relating to individual schools or colleges and their students, is held on a server at each establishment, and it is required to provide controlled access to this information, over the internet, for educational authorities, teachers, governors, parents or students. It will be appreciated that in practice, different levels of access will be provided, appropriate to each user or category of users.

One embodiment of the invention will now be described, with reference to the accompanying which is a schematic diagram of a system according to the invention.

As shown in the drawings, individual school servers indicated at references 2 to 8 store information such as student attendance and performance information, which is required to be accessed periodically, from various PCs or network terminals in different categories such as 10 (representing the LEA), 12 (representing governors), 14 (representing teachers) or 16 (representing parents).

Normally these will be remotely located using the internet but they may of course be connected by an "intranet" or WAN.

A centrally located "portal server" 18 is arranged to receive enquiries from the PCs or terminals 10, 16, whilst the individual servers 2 to 8 will only accept connections from the portal computer 18 itself. In other words, assuming that "internet protocol" is being used for communications, the servers are arranged to reject all IP addresses other than that of the portal.

When an enquiry is received by the portal 18, from one of the remote terminals 10, 12 etc, the user will be required to carry out a log-in procedure, and the portal computer

will then compare the identity of the user, and/or their network station, with an admissible list of users. The portal may also determine, from an internal database, which of the servers 2 to 8 needs to be accessed, and whether access is permitted for that particular enquiring terminal.

If the enquiry is admissible, the portal computer transmits a corresponding message to the required server, which enable it to receive and answer the enquiry. For example, the portal computer may pass a token to the server, and to the enquirer, which enables the server to confirm that it should accept the enquiry by comparing the tokens.

At this point, the server will be enabled to accept a direct communication from the IP address of the enquiring terminal, rather than only via the portal computer, so that the portal computer does not have to handle the entire bandwidth of a large number of enquiries.

In an educational network, authorised users such as LEA's (local educational authorities) can in this way obtain statistical reports on student attendance, grades, behaviour, homework, school performance, etc over the internet using a web browser. When data is required to cover a number of schools, the portal computer may carry a list of a number of appropriate school servers, which any given enquirer is allowed to access. For any particular school, reports may be provided covering various aspects of the performance of the school and the students, such as weekly percentage attendance report for registration groups, attendance reports of a single student over a specified range of weeks, grade average reports etc. Such reports will of course, be made available to both the local educational authority enquirer, and of course, to the school itself. Information relative to the performance of a number of schools in the area, on the other hand, will normally be made available only to the appropriate LEA.

Similarly, reports relating to a particular student will also be made available to parents, so that they will be allowed access to a rather restricted sub-set of the individual school reports.

On each of the servers, a number of software elements will be required:

(1) a database, preferably using SQL (structured query language);

(2) an internet connection which is permanently connected with a static IP configuration;

(3) a "web server" capable of making SSL (secure sockets layer) connections; and

(4) ODBC drivers to provide access to the SQL database.

This will enable the server to return the required data in a form appropriate to the enquiry, e.g. as html.

It will be appreciated that the present invention can confer a number of cost and performance advantages, because there is only one portal server in the whole system whereas there are thousands of school servers. With the preferred arrangement:

(1) The"portal server" can be installed and developed with as high security software as possible as only one is required to benefit all users.

(2) Although the potential bandwidth requirement to service thousands of schools and millions of parents would be enormous, this requirement can be alleviated by using the portal server only in the initial log-in procedures and for authenticating the requests.

(3) Similarly the amount of information stored centrally on the portal server could be very large, if it were required to hold information normally held by thousands of school servers. This also involves additional complications of keeping copies of school server data up to date on the central portal server.

CLAIMS

1. A distributed database system, in which information is held on a plurality of servers in different physical locations, each having a connection to the internet, and an access portal, also connected to the internet, which is adapted to receive incoming enquiries intended for the servers, to authenticate each enquiry, to identify the appropriate server and to establish a connection with it, once the enquiry has been authenticated.

2. A distributed database system according to claim 1 in which a token is passed to the originator and to the appropriate server, after authentication, so that the server can confirm that the enquiry has been authorised, and a direct connection is then established between the originator and the server.

3. A distributed database system according to claim 1 in which the access portal forwards the request to the appropriate server, after authentication, and the response is routed back to the originator via the access portal so that there is no direct connection between the originator and the server.

4. An educational information network comprising a plurality of servers at different educational establishments holding information relating to students and arranged to form a distributed database system in accordance with any of claims 1 to 3.

5. A method of controlling access to a distributed database system in which information is held on a plurality of servers in different physical locations, each having a connection to the internet, the method comprising (a) arranging an access portal to receive all incoming enquiries to the servers of the database; (b) authenticating each enquiry at the access portal; and (c) identifying an appropriate server to deal with the enquiry and establishing a connection with it, after successful authentication of the enquiry.